

Ethik-Richtlinie für Anbieter kritischer digitaler Infrastruktur

Inhaltsverzeichnis

Einleitung

Big Tech als potenzieller Wegbereiter von schweren Umwelt- und Menschenrechtsverstößen	3
Der »ethische Mindeststandard« für Cloud-Anbieter	4

Ethik-Richtlinie

Präambel	5
1. Nutzungsbeschränkung von Cloud-Dienstleistungen	5
1.1 Fossile Brennstoffe & Umweltzerstörung	5
1.2 Menschenrechtsverletzungen	6
1.3 Waffensysteme & Militär	6
1.4 Überwachung, Repression & »Unacceptable Risks« ...	7
1.5 Desinformation & demokratische Integrität	7
2. Faire, ökologische Lieferketten & Transparenz	8
2.1 Ökologische Sorgfaltspflicht & Transparenz	8
2.2 Saubere & faire Hardware-Wertschöpfungskette	8
2.3 Arbeitsschutz für Clickworker	9
3. Politische Integrität & Transparenz über Lobbyismus	9
4. Compliance & Durchsetzung der Richtlinie	9

Big Tech als potenzieller Wegbereiter von schweren Umwelt- und Menschenrechtsverstößen

Big-Tech-Konzerne, insbesondere Anbieter kritischer Cloud-Infrastruktur wie Amazon Web Services (AWS), Microsoft und Google, sind heute die zentralen »Wegbereiter« der modernen Welt. Sie stellen die digitale Infrastruktur bereit – das Fundament, auf dem Regierungen und Wirtschaftsakteure operieren, aber auch der Raum, in dem zwischenmenschliche und gesellschaftliche Interaktion stattfindet. Damit geht eine Machtposition einher, die Risiken birgt und über rein technische Fragen hinausgeht:

- **Ressourcenverbrauch:** Der Betrieb von Cloud-Infrastruktur verbraucht massiv Energie und Rohstoffe, was zunehmend mit internationalen Umweltzielen, wie denen des *Pariser Klimaabkommens* oder dem Ausstieg aus fossilen Brennstoffen, kollidiert.
- **Umwelt- und Menschenrechtsverstöße:** Aktuell profitieren auch Unternehmen, deren Geschäftsmodelle zerstörerische gesamtgesellschaftliche Auswirkungen haben (zum Beispiel Rüstungs-, Entwaldungs- oder fossile Energieunternehmen) von den bereitgestellten IT-Dienstleistungen.
- **Überwachung & militärische Nutzung:** Digitale Infrastruktur kann beispielsweise durch den Einsatz von KI zur Zusammenführung großer Datensätze oder zur Zielerfassung von Drohnen verwendet und so zur Stärkung autoritärer Strukturen oder für völkerrechtswidrige militärische Zwecke missbraucht werden.
- **Systemische Abhängigkeit:** Als »Nadelöhr« entscheiden Cloud-Anbieter indirekt über den Marktzugang von Unternehmen und die Datenhoheit ganzer Volkswirtschaften und deren Bürger:innen.

Big-Tech-Unternehmen, darunter Anbieter von Cloud-Services, sind wie alle Unternehmen keine isolierten wirtschaftlichen Akteure, sondern tragen Verantwortung für ihre Auswirkungen auf Menschenrechte, Arbeitsnormen und die Umwelt entlang der gesamten Wertschöpfungskette. Die Wirtschaftsgeschichte zeigt, dass insbesondere Sektoren mit hoher Innovationsdynamik und systemrelevanten Geschäftsmodellen einer besonderen ethischen Pflicht gegenüber der Gesellschaft unterliegen. Beispielsweise stellt der Gesundheits- und Pharmasektor durch jahrhundertealte Selbstverpflichtungen und strenge Zulassungsverfahren für Medikamente sein Unternehmensmodell in den Dienst der Allgemeinheit und schützt es so vor Missbrauch. Auch der Finanzsektor definiert ökologische und soziale Ausschlusskriterien für Investitionen in den *UN Principles for Responsible Investment (PRI)*. Genauso muss heute auch der Tech-Sektor seiner Rolle und Verantwortung als gemeinwohlfördernder Innovator gerecht werden und ökologische und ethische Mindeststandards einführen, die ein gutes Leben für alle ermöglichen.

Der »ethische Mindeststandard« für Cloud-Anbieter

Mit dem *Digital Services Act (DSA)*, dem *Digital Markets Act (DMA)* und dem *AI Act* hat die EU in den vergangenen Jahren bereits wegweisende Leitplanken zur Regulierung von Tech-Unternehmen und KI-Entwicklungen gesetzt. Dennoch kann staatliche, noch dazu regionale Regulierung allein nicht mit der Geschwindigkeit globaler technologischer Disruption mithalten. Bis die staatliche Regulierung den technologischen Fortschritt einholt, sind branchenweite Selbstverpflichtungen, wie man sie aus dem Finanz- oder Pharmasektor kennt, erforderlich, um die besondere Verantwortung digitaler »Wegbereiter« anzuerkennen.

Insbesondere für Anbieter von Cloud-Infrastruktur besteht eine strukturelle Parallele zum Finanzwesen: Ähnlich wie eine Bank durch Kredite bestimmte Projekte ermöglicht, ermöglicht ein Cloud-Anbieter durch Rechenpower und IT-Dienstleistungen unzählige neue Geschäftsmodelle, wie *Software-as-a-Service (SaaS)*, *Infrastructure-as-a-Service (IaaS)* oder digitale Marktplätze, und erhöht die Effizienz schon bestehender Geschäftsmodelle. Analog zu Finanzinstituten, die die Finanzierung von umstrittenen Waffen, klimaschädlichen Geschäftsmodellen oder von Regenwaldabholzung ausschließen, übertragen die von Greenpeace in diesem Dokument erarbeiteten Ethik-Mindeststandards diese bewährten Prinzipien auf die Anbieter von Cloud-Services. Die hier vorliegende Richtlinie definiert die roten Linien, die Cloud-Infrastruktur-Anbieter ziehen müssen, um sicherzustellen, dass technologischer Fortschritt nicht für reine Profitmaximierung missbraucht wird und zu Lasten des Gemeinwohls erfolgt.

Die folgende ausformulierte Richtlinie für Anbieter kritischer digitaler Infrastruktur dient dazu, diese abstrakten ökologischen und ethischen Mindeststandards in eine operative Realität zu übersetzen, die Mensch und Umwelt achtet und demokratische Strukturen stärkt. Die Richtlinie dient als Vorlage und ist als direkt unterschriftsreife Selbstverpflichtung für Unternehmen konzipiert. Sie zeigt auf, wie Weltmarktführer wie AWS, Microsoft und Google ihre gesellschaftliche Verantwortung nicht nur in Nachhaltigkeitsberichten beteuern, sondern in Form verbindlicher Handlungsrichtlinien tief in ihr Geschäftsmodell – von der Kundenauswahl über die Ressourcennutzung bis hin zur politischen Einflussnahme – integrieren können. Ein solches Bekenntnis wäre der notwendige Schritt, um von einem reinen Technologie-Anbieter zu einem verantwortungsvollen Akteur einer demokratischen und nachhaltigen digitalen Zukunft für alle zu werden.

PRÄAMBEL

Als Unternehmen, das zu den weltweit führenden Anbietern von Cloud-Infrastruktur zählt, erkennen wir an, dass Technologie nicht neutral ist, sondern ihr Einsatz mit gesellschaftlicher Verantwortung einhergeht. Wir übernehmen die damit verbundene Verantwortung und verpflichten uns mit der vorliegenden Richtlinie, verbindliche Maßnahmen zu ergreifen, die sicherstellen, dass die von uns bereitgestellten Dienstleistungen nicht missbraucht werden, um der Umwelt zu schaden, Menschenrechte zu gefährden oder Demokratien zu untergraben. Diese Richtlinie stellt das verantwortungsvolle wirtschaftliche Handeln innerhalb der planetaren Grenzen sicher und gilt für alle Geschäftsbereiche, Tochtergesellschaften und Partnerschaften.

1. NUTZUNGSBESCHRÄNKUNG VON CLOUD-DIENSTLEISTUNGEN

Wir beschränken die Nutzung der bereitgestellten Infrastruktur (Rechenleistung, Speicher, Cloud-Services) und unterlassen eine etwaige gemeinsame Produktentwicklung in folgenden Bereichen:

1.1 Fossile Brennstoffe & Umweltzerstörung

Im Einklang mit internationalen Umweltgesetzen, wie dem *Pariser Klimaabkommen*, dem *Übereinkommen über die biologische Vielfalt (CBD)*, dem *UN-Hochseeschutzabkommen* und der *EU-Entwaldungsverordnung (EUDR)*, wird die Bereitstellung von Infrastruktur für folgende Unternehmen und Anwendungszwecke ausgeschlossen:

- **Kohleentwickler und -verstromer:** Kohleförderer mit Expansionsplänen entlang der gesamten Kohlewertschöpfungskette (gemäß [Global Coal Exit List](#) von Urgewald).
- **Expandierende Öl- und Gasunternehmen:** Unternehmen, die weiter in fossile Brennstoffe (Ausbau, Upstream und Midstream), den Bau von Öl- und Gaspipelines für neue fossile Reserven sowie in neue Terminals für den Export/Import von LNG expandieren (gemäß [Global Oil and Gas Exit List](#) von Urgewald).
- **Unkonventionelle Öl- und Gasförderung:** Unternehmen, die Fracking, Ölsand-, Schieferöl- sowie Arktis- und Tiefseeförderung (gemäß [AMAP-Definition](#)) betreiben.
- **Unternehmen mit schwerwiegenden Umwelt-Kontroversen:** Unternehmen, die schwere, irreversible Schäden an Ökosystemen anrichten, wie zum Beispiel durch Tiefseebergbau, durch industrielle Aktivitäten wie der Einleitung von Chemie und Abfällen oder durch Katastrophen im Bergbau (Dammbrüche).
- **Entwaldungsunternehmen:** Firmen, die nachweislich in Entwaldung oder illegale Landnahme involviert sind, sofern sie keine lückenlose, verifizierbare Rückverfolgbarkeit ihrer Lieferkette nachweisen.
- **Täuschungssysteme:** Systeme zur Verschleierung der Herkunft von Agrarrohstoffen («Cattle Laundering») aus geschützten Gebieten (zum Beispiel Amazonas, Cerrado).

1.2 Menschenrechtsverletzungen

Im Einklang mit der *UN-Menschenrechtserklärung*, den *UN-Leitprinzipien für Wirtschaft und Menschenrechte* sowie der *UN-Erklärung über die Rechte indigener Völker (UNDRIP)* wird die Bereitstellung von Infrastruktur für folgende Unternehmen und Anwendungszwecke ausgeschlossen:

- **Schwerwiegende Menschenrechts-Kontroversen:** Der Einsatz von Kinderarbeit und Zwangsarbeit, prekäre Arbeitsbedingungen, die Unterdrückung der Vereinigungsfreiheit sowie systematische Diskriminierung.
- **Verletzung der persönlichen Integrität:** Neben physischer und psychischer Gewalt auch digitale Gewalt in Form von nicht-einvernehmlichen pornografischen Inhalten, darunter insbesondere durch generative KI erzeugte Deepfakes.
- **Verletzung indigener Rechte:** Aktivitäten, die zur widerrechtlichen Aneignung von Land, zur Zerstörung von kulturellem Erbe oder zur Ausbeutung von Ressourcen in Gebieten indigener Völker ohne deren freie, vorherige und informierte Zustimmung (FPIC) beitragen.

1.3 Waffensysteme & Militär

Im Einklang mit internationalen Konventionen zu geächteten Waffensystemen und dem *EU AI Act* wird folgende militärische Nutzung von Cloud-Infrastruktur ausgeschlossen:

- **Letale Autonome Waffensysteme (LAWS):** Die Entwicklung, Herstellung und der Einsatz von Waffensystemen, die ohne wesentliche menschliche Kontrolle Ziele auswählen und angreifen (gemäß Vorschlag der NGO Coalition »Campaign to Stop Killer Robots«).
- **Kinetische Angriffsplanung:** Die direkte Zielerfassung oder operative Durchführung kinetischer Angriffe.
- **Kontroverse Waffengattungen:** Die Entwicklung und Nutzung von Streumunition, chemischen/biologischen Waffen, Antipersonenminen sowie von blind-machenden Laserwaffen, Atomwaffen, Brandwaffen mit weißem Phosphor, radiologischen Waffen, Waffen aus abgereichertem Uran und nicht entdeckbarer Splittermunition.

1.4 Überwachung, Repression & »Unacceptable Risks«

Die Nutzung von Cloud-Infrastruktur (nicht nur KI-bezogen) für folgende Anwendungen, die gemäß *EU-AI Act* Artikel 5 ein unannehmbares Risiko darstellen, wird untersagt:

- **Manipulative Techniken:** Die Nutzung unterschwelliger (subliminaler) oder gezielt manipulativer Techniken, um das Verhalten einer Person so zu beeinflussen, dass ihr oder anderen Personen ein erheblicher Schaden zugefügt wird.
- **Ausnutzung von Schutzbedürftigkeit:** Das gezielte Ausnutzen von Schwächen von Personen aufgrund ihres Alters, einer Behinderung oder einer spezifischen sozialen oder wirtschaftlichen Situation, um deren Verhalten schädlich zu beeinflussen.
- **Social Scoring:** Die Bewertung der Vertrauenswürdigkeit von Bürger:innen, die zu diskriminierenden Konsequenzen führt.
- **Predictive Policing:** Die Berechnung der Wahrscheinlichkeit von Straftaten basierend auf Profiling oder Persönlichkeitsmerkmalen.
- **Biometrisches Scraping:** Das ungezielte Auslesen (Scraping) von Personenbildern aus dem Internet oder von Videoüberwachung, um Datenbanken für die Gesichtserkennung zu erstellen oder zu erweitern.
- **Emotionserkennung:** Die Erkennung von Emotionen am Arbeitsplatz oder in Bildungseinrichtungen.
- **Biometrische Kategorisierung:** Die Sortierung von Menschen an Landesgrenzen in bestimmte Kategorien (Ethnizität, Religion, sexuelle und politische Orientierung), basierend auf biometrischen Daten.
- **Biometrische Fernidentifizierung:** Die Echtzeit-Gesichtserkennung im öffentlichen Raum durch staatliche oder private Akteure.
- **Grenzüberwachung:** Die Verhaltensanalyse von Geflüchteten oder Prognosen von Migrationsbewegungen, die zur völkerrechtswidrigen Abweisung (Pushbacks) führen könnten.

1.5 Desinformation & demokratische Integrität

Die Nutzung von Cloud-Infrastruktur wird für folgende Anwendungen untersagt, sofern sie demokratische Strukturen nachweislich untergraben:

- **Deepfakes & Transparenz:** Die Erstellung von manipulierten Inhalten (Audio/Video), die ohne Kennzeichnung darauf abzielen, Wahlen zu beeinflussen oder die öffentliche Meinung zu täuschen.
- **Politische Gruppen:** Organisationen, deren Ziel die Zersetzung der freiheitlich-demokratischen Grundordnung ist.

2. FAIRE, ÖKOLOGISCHE LIEFERKETTEN & TRANSPARENZ

Basierend auf den Sorgfaltspflichten der *EU-Lieferkettenrichtlinie (CSDDD)* verpflichten wir uns dazu, unsere Marktmacht für eine faire, ökologische Lieferkette und eine gerechte Infrastruktur einzusetzen, die den Schutz der betroffenen Menschen ins Zentrum stellt. Wir erkennen an, dass technologischer Fortschritt untrennbar mit den Lebensgrundlagen lokaler Gemeinschaften verbunden ist. Von der Strom- und Wasserversorgung der Rechenzentren über die Minen zur Rohstoffgewinnung bis hin zur digitalen Arbeit der Clickworker tragen wir die Verantwortung dafür, dass Fortschritt nicht auf Kosten der Schwächsten in der Lieferkette erfolgt.

2.1 Ökologische Sorgfaltspflicht & Transparenz

- **24/7 Renewable Energy:** Neue Rechenkapazitäten ausschließlich mit Strom aus Erneuerbaren Energien (EE) betreiben, wobei Zertifikate für Grünstrom nicht ausreichen. Erneuerbare umfassen Wind-, Solar-, Geothermie- und Wasserkraft. Atomenergie fällt nicht darunter. Auch Backup-Lösungen müssen auf EE basieren.
- **Beitrag zur Netzstabilisierung:** Lösungen wie Demand-Side-Management (flexibles Hoch- und Herunterfahren) sowie Batteriespeicher nutzen.
- Einsatz von **geschlossenen Kühlkreisläufen** oder Trockenkühlungen in allen Regionen mit Wasserstress. Es wird kein Trinkwasser zur Kühlung eingesetzt.
- **Abwärmennutzung:** Mindestens 25 Prozent der Abwärme muss weiterverwertet werden, perspektivisch wird eine 80-prozentige Nutzung angestrebt.
- **Offenlegungspflicht:** Alle relevanten Umweltkennzahlen zu Energie- und Wasserverbräuchen sowie zum eingesetzten Strommix, sowohl in aggregierter Form als auch auf Standortebene, werden berichtet.
- **Transparenz über Workloads:** Bereitstellung von nachprüfbaren, modellbasierten Schätzungen des CO₂- und Wasser-Fußabdrucks jeder Recheninstanz eines Workloads für Kund:innen.

2.2 Saubere & faire Hardware-Wertschöpfungskette

- **Risikomanagement & Transparenz:** Bereitstellung einer umfassenden Risikokarte der Hardware-Lieferkette (vom Bergbau bis zur Fertigung), die ökologische Schäden identifiziert und die Emissionen aller IT-Komponenten quantifiziert.
- **Aktive Sorgfaltspflicht (Leverage):** Sicherstellung der Compliance durch verbindliche Vertragsklauseln, die Lieferanten zur Einhaltung von EU-Umwelt- und Menschenrechtsstandards verpflichten, sowie technische Unterstützung für diese Lieferanten.
- **Abhilfe & Betroffenenbeteiligung:** Implementierung transparenter Abhilfeprozesse bei Verstößen gegen die Richtlinie, die den Schutz von Umweltaktivist:innen sowie die Entschädigung betroffener Gemeinden (Landverlust, Gesundheit) unter direkter Einbeziehung der lokalen Akteure garantieren.
- **Zirkularität & E-Waste:** Nachweis bis 2030, dass Hardware nach dem Austausch primär in »Second Life«-Programmen weiterverwendet oder zu mindestens 90 Prozent stofflich recycelt wird.
- **Rechenschaftslegung:** Veröffentlichung einer jährlichen Due-Diligence-Erklärung, die Fortschritte bei der Risikoprävention, der Scope-3-Reduktion und den Recyclingquoten prüfbar dokumentiert.

2.3 Arbeitsschutz für Clickworker

- **Transparenz der digitalen Lieferkette:** Transparenz über die geografische Verteilung und Arbeitsstandards von Clickwork. Keine Inanspruchnahme von Leistungen, bei denen Anhaltspunkte für Kinderarbeit, Zwangsarbeit oder moderne Sklaverei (gemäß *ILO-Kernarbeitsnormen* und dem *UK Modern Slavery Act*) vorliegen. Dies gilt insbesondere für die Vergabe von Microtasks in Hochrisikoregionen ohne nachweisbare Kontrollmechanismen der Plattform.
- **Einhaltung der ILO-Prinzipien sowie der nationalen Arbeitsgesetze** für alle Clickworker, die für oder im Auftrag von uns tätig sind. Dazu zählen eine faire Vergütung, die sich an den lokalen Standards für existenzsichernde Löhne orientiert, die Vereinigungsfreiheit und das Recht der Arbeitnehmer:innen auf gewerkschaftliche Organisation sowie eine unabhängige Überprüfung der Arbeitsbedingungen auf der Plattform.

3. POLITISCHE INTEGRITÄT & TRANSPARENZ ÜBER LOBBYISMUS

- **Verzicht auf Aushöhlung bestehender Klimaschutz- und Tech-Regulierung:** Verzicht auf die aktive Bekämpfung von Klima-/Umwelt- und Tech-Regulierung, darunter die *EU-Energieeffizienzrichtlinie (EED)*, der *Digital Markets Act (DMA)* und der *Digital Services Act (DSA)*.
- **Transparenz über Netzwerk und Lobbyausgaben:** Jährliche Veröffentlichung aller Lobbyausgaben, aufgeschlüsselt nach internem Personal, Lobbyagenturen, Industrieverbänden, Think-Tanks, Image-Kampagnen und weiteren lokalen Initiativen wie Events oder Sponsorings.
- **Transparenz über persönliche Treffen:** Veröffentlichung aller Protokolle von hochrangigen Treffen mit EU-Kommissar:innen und Abgeordneten. Außerdem über die gesetzliche Pflicht hinaus die Angabe aller Treffen mit politischen Akteur:innen im Lobbyregister.

4. COMPLIANCE & DURCHSETZUNG DER RICHTLINIE

Eine Richtlinie ohne Prozesse zur Überwachung ist wirkungslos. Deshalb braucht es effiziente interne Kontrollmechanismen.

- **Prozess zu Umsetzung und Monitoring der Ethik-Richtlinie verankern:** Es werden keine Geschäftsbeziehungen mit Kund:innen aufgenommen, deren Tätigkeiten gegen die in Kapitel 1 festgehaltenen Regeln verstoßen. Ingenieur:innen erhalten das vertraglich zugesicherte Recht, die Arbeit an Projekten zu verweigern, die gegen diese Richtlinie verstoßen, ohne berufliche Nachteile.
- **Grundrechte-Folgenabschätzung:** Wir verpflichten uns, von allen Kund:innen, die Hochrisiko-Systeme gemäß *EU AI Act* betreiben, den Nachweis einer durchgeführten Grundrechte-Folgenabschätzung zu verlangen, unabhängig davon, ob es sich um staatliche oder private Stellen handelt.
- **Ethik-Rat:** Einberufung eines unabhängigen, externen Ethik-Rats mit Vertreter:innen aus der Zivilgesellschaft und Wissenschaft. Dieser veröffentlicht offizielle Empfehlungen zur Beendigung der Zusammenarbeit mit kritischen Kund:innen.



Kein Geld von Industrie und Staat

Greenpeace arbeitet international und kämpft mit gewaltfreien Aktionen für den Schutz der Lebensgrundlagen. Ziel ist es, Umweltzerstörung zu verhindern, Verhaltensweisen zu ändern und Lösungen durchzusetzen. Greenpeace ist überparteilich und völlig unabhängig von Politik und Wirtschaft. Mehr als 620.000 Fördermitglieder in Deutschland spenden an Greenpeace und gewährleisten damit unsere tägliche Arbeit zum Schutz der Umwelt, der Völkerverständigung und des Friedens.

Wir holen uns das Internet zurück. Der Widerstand wächst. Weltweit.



► **Schließ dich uns an!**

Trag dich ein und sei Teil der Bewegung.
act.greenpeace.de/bigtech

Impressum

Greenpeace e.V. Hongkongstraße 10, 20457 Hamburg, T 040 30618-0, mail@greenpeace.de, greenpeace.de,
Politische Vertretung Berlin Marienstraße 19–20, 10117 Berlin, T 030 308899-0 **V. i. S. d. P.** Marie Kuhn
Text Marie Kuhn **Titel / Cover** tuckow.studio **Fotos** © istockphoto [M] **Gestaltung** Andrea Bayer **Stand** 05 / 2026